AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A stream enciphering method for generating a cryptographic code by carrying out exclusive-OR operations between a plaintext code which is a secrecy object and a PN signal, wherein said PN signal is formed such that the least common multiple of the length of a PN signal cycle and the basic processing unit of said plaintext code has a ~~predetermined~~ large value relative to said PN signal cycle.

2. (Currently Amended) A deciphering method for deciphering a cryptographic code to a plaintext code which is a secrecy object, the cryptographic code being enciphered by a stream enciphering method for generating the cryptographic code by carrying out exclusive-OR operations between the plaintext code and a PN signal being formed such that the least common multiple of the length of a PN signal cycle and the basic processing unit of said plaintext code has a ~~predetermined~~ large value relative to said PN signal cycle, wherein

said cryptographic code is restored to an original plaintext code by carrying out exclusive-OR operations by obtaining synchronism between said cryptographic code and a same PN signal as said PN signal.

3. (Currently Amended) A cryptographic communication system constituted so as to be capable of achieving cryptographic communication between a transmitter side and a receiver side, wherein

said transmitter side comprises:

a plaintext storage means for storing a plaintext code which is a secrecy object by each basic processing unit;

a transmitter side PN signal storage means for storing a PN signal which is formed such that the least common multiple of the length of a PN signal cycle and the basic processing unit of said plaintext code has a ~~predetermined~~ large value relative to said PN signal cycle;

an enciphering means for generating a cryptographic code by carrying out exclusive-OR operations between the plaintext code stored in said plaintext storage means and the PN signal in said transmitter side PN signal storage means; and

a transmitting means for transmitting the cryptographic code generated by said enciphering means to the receiver side, and

said receiver side comprises:

a receiving means for receiving the cryptographic code transmitted from said transmitting means;

a cipher text storage means for storing the cryptographic code received by said receiving means by each basic processing unit;

a receiver side PN signal storage means for storing a same PN signal as the PN signal stored in said transmitter side PN signal storage means; and

a deciphering means for deciphering the cryptographic code to an original plaintext code by carrying out exclusive-OR operations by obtaining synchronism between the cryptographic code stored in said cipher text storage means and the PN signal stored in said receiver side PN signal storage means.

4. (New) The stream enciphering method according to claim 1, wherein the basic processing unit of said plaintext code is an even number.

5. (New) The stream enciphering method according to claim 4, wherein the basic processing unit of said plaintext code is multiples of 8 bits.

6. (New) The stream enciphering method according to claim 1, wherein a bit length of the PN signal cycle is an odd number.

7. (New) The stream enciphering method according to claim 6, wherein the bit length of the PN signal cycle is one of 7, 15, 23 and 63.

8. (New) The deciphering method according to claim 2, wherein the basic processing unit of said plaintext code is an even number.

9. (New) The deciphering method according to claim 8, wherein the basic processing unit of said plaintext code is multiples of 8 bits.

10. (New) The deciphering method according to claim 2, wherein a bit length of the PN signal cycle is an odd number.

11. (New) The deciphering method according to claim 10, wherein the bit length of the PN signal cycle is one of 7, 15, 23 and 63.

12. (New) The cryptographic communication system according to claim 3, wherein the basic processing unit of said plaintext code is an even number.

13. (New) The cryptographic communication system according to claim 12, wherein the basic processing unit of said plaintext code is multiples of 8 bits.

14. (New) The cryptographic communication system according to claim 3, wherein a bit length of the PN signal cycle is an odd number.

15. (New) The cryptographic communication system according to claim 14, wherein the bit length of the PN signal cycle is one of 7, 15, 23 and 63.